Remarks by Rand Beers
White House Deputy Homeland Security Advisor
At the U.S. Department of Justice
On the DOJ/FTC Announcement on Cybersecurity
April 10, 2014

AS PREPARED FOR DELIVERY

Thank you… and good morning to you all.

I'm Rand Beers, Deputy Assistant to the President for Homeland Security. My title doesn't have the word "cyber" in it, but given the importance of this issue to the Administration, it probably should.

You all know as well as I do that cyber threats are increasing at the same time that more and more critical industries are using the Internet to store information and deliver services. Combined with easy-to-use malware and malicious actors willing to be destructive, the cybersecurity landscape is only becoming more challenging.

But it's not all bad news. In February, the Administration launched the Cybersecurity Framework – an industry-led initiative borne out of the President's executive order last year. The development of that framework, designed to raise the level of cybersecurity across our country, and the implementation efforts that are moving forward at network speed, are a great example of what we can do when government and industry come together to meet this threat head on.

Today, I'm here to help roll out another big win.

It's no secret that some companies worry about violating antitrust laws if they share cybersecurity information with their competitors. Everyone from the CEOs that sit on the President's National Security Telecommunications Advisory to the House Republican Cybersecurity Task Force have identified antitrust as a barrier to effective cybersecurity information sharing.

So the good news today is that the Department of Justice and the Federal Trade Commission, the Federal experts in antitrust law, have released new guidance emphasizing that antitrust is not, should not be a worry when it comes to legitimate cybersecurity information sharing.

Laying concerns over antitrust liability to rest addresses one perceived barrier to increased information sharing. Over the next year, we will continue to knock down these barriers – real or perceived. Our hope is that we can turn the conversation from what we can't do to secure the nation to figuring out what we can do.

Networks can be more secure. We can maintain our privacy. Companies can better protect consumer data and their intellectual property.

We know this because there are some companies and government agencies that are getting much better at cybersecurity.

In the process of getting better at defending their networks, government and industry have identified some necessary steps to achieving effective cybersecurity. I'll lay out one key finding from those efforts and then I'll talk about how the antitrust guidelines fit in. The key finding is this: companies with effective cybersecurity practices have robust information sharing efforts and they are all doing the same three things to lay the ground work for that sharing.

First, they have identified the cybersecurity best practices for their industry and they are evaluating their cybersecurity against those benchmarks. They are using these practices to make decisions about the capabilities they must develop. If a company or organization is inexperienced in this area, then the Cybersecurity Framework I mentioned earlier is a good place to start.

Second, they are using continuous diagnostic and monitoring techniques to make sure they are consistently in compliance with these standards in real time. And they take corrective action to fix the problems those monitoring systems reveal.

Third, their security operations centers have developed advanced capabilities to identify unknown threats at their network perimeters and to hunt for those threats within their networks.

With these programs and capabilities in place, when companies identify previously unknown threats on their networks, they share the indicators of that activity with their trusted partners in standardized formats.

In turn, when their information sharing partners discover similar activity, these companies receive information from them and use it to defend their own networks.

In this way, information sharing turns the conventional wisdom that the attacker has the advantage in cyberspace on its head.

Without effective information sharing, an attacker can send the same spearphishing message with the same malware to thousands of different targets, assuming that some will identify and stop the attack but most will not.

If companies are sharing information with each other, detection by one company can thwart the attack for many, creating the equivalent of herd immunity in cyberspace.

While this sharing occurs in limited ways by a number of companies today, this kind of sharing needs to expand dramatically. That is why today's announcement is so important. It will be a key enabler in driving that expansion of private-to-private sharing. Let me be clear: The Federal government wants companies to communicate with each other about threats. We are not standing in the way; in fact, we are doing just the opposite. We are actively encouraging it.

Over the next year, we will continue efforts to expand cybersecurity information in all the ways we can, whether government-to-private, private-to-private, within the Federal government, among our international partners, or with State and local governments. We will work with our partners in the private sector to help strengthen the network of information sharing organizations that can make cybersecurity information sharing fast, secure, and privacy enhancing. Many private and non-profit networks are already at work in this space. We need more of them, we need them linked together, and we need more individual companies actively participating in them.

Lastly, we intend to keep up our efforts at outreach, particularly to the general counsels, the CEOs, and the CIOs out there. For general counsels that have previously told their CEOs that sharing information is something companies should be wary of because of antitrust concerns, we encourage them to take a look at today's guidance and reevaluate their position. For CEOs, we urge them to send the guidance to their GCs and ask them to review it. To the CIOs, we urge you to take this opportunity to advocate for increased information sharing – it will only make your job easier.

I'm sorry that I need to leave before my colleagues speak. I actually have another cybersecurity event to attend across town.

Let me close by thanking the Department of Justice for hosting us here today and for their work, together with the FTC, to provide this clear and authoritative guidance.

###